Version 7.11

Part No. NN46110-510.01.01
325391-A
Document status: Standard
December 2008

600 Technology Park Drive
Billerica, MA 01821-4130

Nortel VPN Client Configuration — FIPS 140-2

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Nortel Networks Inc.

The software described in this document is furnished under a license agreement and may be used only in accordance with the terms of that license. The software license agreement is included in this document.

Trademarks

Nortel Networks, the Nortel Networks logo, the Globemark, Unified Networks, and Contivity are trademarks of Nortel Networks.

ActivCard is a trademark of ActivCard Incorporated.

Adobe and Acrobat Reader are trademarks of Adobe Systems Incorporated.

America Online is a trademark of America Online, Inc.

Datakey is a trademark of Datakey, Inc.

Entrust is a trademark of Entrust Technologies Inc.

iPass is a trademark of iPass Inc.

Java and Sun Microsystems are trademarks of Sun Microsystems, Inc.

Microsoft and Windows are trademarks of Microsoft Corporation.

Netscape and Netscape Navigator are trademarks of Netscape Communications Corporation.

SecurID is a trademark of RSA Security Inc.

VeriSign is a trademark of VeriSign Incorporated.

The asterisk after a name denotes a trademarked item.

Restricted rights legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of conditions

In the interest of improving internal design, operational function, and/or reliability, Nortel Networks Inc. reserves the right to make changes to the products described in this document without notice.

Nortel Networks Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Nortel Networks Inc. software license agreement

This Software License Agreement (“License Agreement”) is between you, the end-user (“Customer”) and Nortel Networks Corporation and its subsidiaries and affiliates (“Nortel Networks”). PLEASE READ THE FOLLOWING CAREFULLY. YOU MUST ACCEPT THESE LICENSE TERMS IN ORDER TO DOWNLOAD AND/OR USE THE SOFTWARE. USE OF THE SOFTWARE CONSTITUTES YOUR ACCEPTANCE OF THIS LICENSE AGREEMENT. If you do not accept these terms and conditions, return the Software, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

“Software” is owned or licensed by Nortel Networks, its parent or one of its subsidiaries or affiliates, and is copyrighted and licensed, not sold. Software consists of machine-readable instructions, its components, data, audio-visual content (such as images, text, recordings or pictures) and related licensed materials including all whole or partial copies. Nortel Networks grants you a license to use the Software only in the country where you acquired the Software. You obtain no rights other than those granted to you under this License Agreement. You are responsible for the selection of the Software and for the installation of, use of, and results obtained from the Software.

1. Licensed Use of Software. Nortel Networks grants Customer a nonexclusive license to use a copy of the Software on only one machine at any one time or to the extent of the activation or authorized usage level, whichever is applicable. To the extent Software is furnished for use with designated hardware or Customer furnished equipment (“CFE”), Customer is granted a nonexclusive license to use Software only on such hardware or CFE, as applicable. Software contains trade secrets and Customer agrees to treat Software as confidential information using the same care and discretion Customer uses with its own similar information that it does not wish to disclose, publish or disseminate. Customer will ensure that anyone who uses the Software does so only in compliance with the terms of this Agreement. Customer shall not a) use, copy, modify, transfer or distribute the Software except as expressly authorized; b) reverse assemble, reverse compile, reverse engineer or otherwise translate the Software; c) create derivative works or modifications unless expressly authorized; or d) sublicense, rent or lease the Software. Licensors of intellectual property to Nortel Networks are beneficiaries of this provision. Upon termination or breach of the license by Customer or in the event designated hardware or CFE is no longer in use, Customer will promptly return the Software to Nortel Networks or certify its destruction. Nortel Networks may audit by remote polling or other reasonable means to determine Customer’s Software activation or usage levels. If suppliers of third party software included in Software require Nortel Networks to include additional or different terms, Customer agrees to abide by such terms provided by Nortel Networks with respect to such third party software.

2. Warranty. Except as may be otherwise expressly agreed to in writing between Nortel Networks and Customer, Software is provided “AS IS” without any warranties (conditions) of any kind. NORTEL NETWORKS DISCLAIMS ALL WARRANTIES (CONDITIONS) FOR THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF NON-INFRINGEMENT. Nortel Networks is not obligated to provide support of any kind for the Software. Some jurisdictions do not allow exclusion of implied warranties, and, in such event, the above exclusions may not apply.

3. **Limitation of Remedies.** IN NO EVENT SHALL NORTEL NETWORKS OR ITS AGENTS OR SUPPLIERS BE LIABLE FOR ANY OF THE FOLLOWING: a) DAMAGES BASED ON ANY THIRD PARTY CLAIM; b) LOSS OF, OR DAMAGE TO, CUSTOMER'S RECORDS, FILES OR DATA; OR c) DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), WHETHER IN CONTRACT, TORT OR OTHERWISE (INCLUDING NEGLIGENCE) ARISING OUT OF YOUR USE OF THE SOFTWARE, EVEN IF NORTEL NETWORKS, ITS AGENTS OR SUPPLIERS HAVE BEEN ADVISED OF THEIR POSSIBILITY. The forgoing limitations of remedies also apply to any developer and/or supplier of the Software. Such developer and/or supplier is an intended beneficiary of this Section. Some jurisdictions do not allow these limitations or exclusions and, in such event, they may not apply.

4. **General**

   a. If Customer is the United States Government, the following paragraph shall apply: All Nortel Networks Software available under this License Agreement is commercial computer software and commercial computer software documentation and, in the event Software is licensed for or on behalf of the United States Government, the respective rights to the software and software documentation are governed by Nortel Networks standard commercial license in accordance with U.S. Federal Regulations at 48 C.F.R. Sections 12.212 (for non-DoD entities) and 48 C.F.R. 227.7202 (for DoD entities).

   b. Customer may terminate the license at any time. Nortel Networks may terminate the license if Customer fails to comply with the terms and conditions of this license. In either event, upon termination, Customer must either return the Software to Nortel Networks or certify its destruction.

   c. Customer is responsible for payment of any taxes, including personal property taxes, resulting from Customer's use of the Software. Customer agrees to comply with all applicable laws including all applicable export and import laws and regulations.

   d. Neither party may bring an action, regardless of form, more than two years after the cause of the action arose.

   e. The terms and conditions of this License Agreement form the complete and exclusive agreement between Customer and Nortel Networks.

   f. This License Agreement is governed by the laws of the country in which Customer acquires the Software. If the Software is acquired in the United States, then this License Agreement is governed by the laws of the state of New York.

Contents

Figures 7

Preface 9

Before you begin 9
Text conventions 9
Acronyms 10
Related publications 11
How to get help 11
    Finding the latest updates on the Nortel Web site 12
    Getting help from the Nortel Web site 12
    Getting help over the phone from a Nortel Solutions Center 13
    Getting help from a specialist by using an Express Routing Code 13
    Getting help through a Nortel distributor or reseller 13

New in this release. 15

    Features 15
    Other changes 15

Configuring FIPS mode 17

Self tests 17
    Initialization self tests 18
    Self integrity check 18
    Known answer tests 19
    FIPS mode status 19
    Continuous random number generator (RNG) test 20
    Split tunneling mode 21
    Logging 21
    Supported DH groups and ciphers 23
    RSA and MSCAPI 23
Disabling FIPS mode 24

Index 25

Figures

Figure 1 Power-up self test 18
Figure 2 Self test failure 18
Figure 3 Status in Help About 19
Figure 4 Status box 20

Preface

This guide provides information about how to configure the Nortel VPN Client to operate in FIPS 140-2 compliant mode.

This guide describes the Nortel VPN Client only in the context of configuring it for FIPS. For more information about Nortel VPN Client software documentation, see *Nortel VPN Router Configuration — Client* Version 7.01 (NN46110-306) 311644-K Rev 02.

Before you begin

This guide is for network managers who are responsible for setting up and configuring the Nortel VPN Client for FIPS 140-2. This guide assumes that you have the following background:

- Experience with system administration
- Familiarity with network management
- Knowledge of FIPS concepts and procedures

Text conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is **`ping`** *`<ip_address>`*, you enter **`ping 192.32.10.12`**

`bold Courier text`	Indicates command names and options and text that you need to enter. Example: Use the **`show health`** command.
brackets ([ ])	Indicate optional elements in syntax descriptions. Do not type the brackets when entering the command. Example: If the command syntax is **`show ntp`** `[`**`associations`**`]`, you can enter either **`show ntp`** or **`show ntp associations`**.
italic text	Indicates new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is **`ping`** *`<ip_address>`*, *`ip_address`* is one variable and you substitute one value for it.
`plain Courier text`	Indicates command syntax and system output, for example, prompts and system messages. Example: `File not found.`
separator (>)	Shows menu paths. Example: Choose Status > Health Check.

Acronyms

This guide uses the following acronyms:

3DES	Triple DES
AES	Advanced Encryption Standard
AH	Authentication Header
DES	Data Encryption Standard
FIPS	Federal Information Processing Standards
HMAC	Hashing Message Authentication Code
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol

IPsec	Internet Protocol Security
KAT	known answer test
MD5	Message Digest 5
NIST	National Institute of Standards and Technology

Related publications

For complete information about installing and configuring the Nortel VPN Client, refer to the following publications (included on the FIPS software CD):

- Nortel VPN Client release notes
- Nortel VPN Router Configuration — Client
- Using Nortel Secure IP Services Gateways In FIPS Mode.

You can print selected technical manuals and release notes free, directly from the Internet. Go to www.nortel.com/documentation, find the product for which you need documentation, and locate the specific category and model, or version, for your hardware or software product. Use Adobe Reader to open the manuals and release notes, search for the sections you need, and print them on most standard printers. Go to the Adobe Systems Web site at www.adobe.com to download a free copy of the Adobe Reader.

How to get help

This section explains how to get help for Nortel products and services.

Finding the latest updates on the Nortel Web site

The content of this documentation was current at the time the product was released. To check for updates to the latest documentation and software for Client, click one of the following links:

Link to	Takes you directly to the
Latest software	Nortel page for **VPN Client** software located at: http://support.nortel.com/go/main.jsp?cscat=SOFTWARE&resetFilter=1&poid=10621
Latest documentation	Nortel page for **VPN Client** documentation located at: http://support.nortel.com/go/main.jsp?cscat=DOCUMENTATION&resetFilter=1&poid=10621

Getting help from the Nortel Web site

The best way to get technical support for Nortel products is from the Nortel Technical Support Web site:

www.nortel.com/support

This site provides quick access to software, documentation, bulletins, and tools to address issues with Nortel products. From this site, you can:

- download software, documentation, and product bulletins
- search the Technical Support Web site and the Nortel Knowledge Base for answers to technical issues
- sign up for automatic notification of new software and documentation for Nortel equipment
- open and manage technical support cases

Getting help over the phone from a Nortel Solutions Center

If you do not find the information you require on the Nortel Technical Support Web site, and you have a Nortel support contract, you can also get help over the phone from a Nortel Solutions Center.

In North America, call 1-800-4NORTEL (1-800-466-7835).

Outside North America, go to the following web site to obtain the phone number for your region:

www.nortel.com/callus

Getting help from a specialist by using an Express Routing Code

To access some Nortel Technical Solutions Centers, you can use an Express Routing Code (ERC) to quickly route your call to a specialist in your Nortel product or service. To locate the ERC for your product or service, go to:

www.nortel.com/erc

Getting help through a Nortel distributor or reseller

If you purchased a service contract for your Nortel product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller.

New in this release

The following sections details what is new in *Nortel VPN Client Configuration — FIPS 140-2*. (NN46110-510).

- “Features
- “Other changes

Features

There are no new features in this release.

Other changes

There are no other changes in this release.

Configuring FIPS mode

The Nortel VPN client can run in normal operating mode or in FIPS operating mode. Version 7.11 has FIPS enabled by default. In FIPS operating mode, the Nortel VPN client meets all requirements for FIPS 140-2. (You can find publications for 140-2 and related information at the http://csrc.nist.gov/cryptval/ URL. For the list of Nortel Networks security policies, click on Validation Lists in the left column of the page. For further information, see *Using Nortel Secure IP Services Gateways In FIPS Mode*.

Whenever you are using vendor products such as, for example, MSCAPI and RSA, you must ensure that those products are also FIPS certified. To check for the current information regarding regarding those compliances, see http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2008.htm.

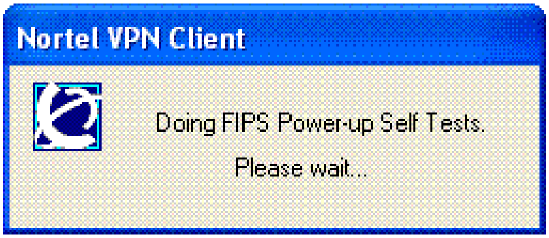
Self tests

To prevent any secure data being released, it is important to test the cryptographic components of a security module to ensure that all components are functioning correctly. The client contains self-tests that are run during startup and periodically during operation.

Initialization self tests

When you enable FIPS mode, the client performs startup self-tests (Figure 1).

Figure 1 Power-up self test



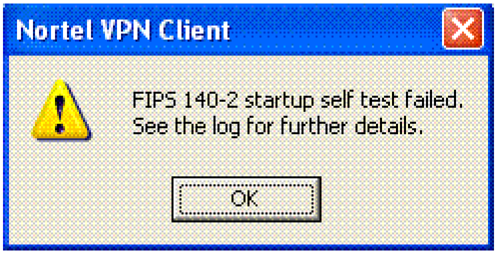
Doing FIPS Power-up Self Tests.

Please wait...

The self tests take approximately 2 seconds on a typical machine (1.8 GHz), but could take as long as 16 seconds on a slow machine.

If any self test fails, the details of the failure are placed into the log and a message indicates a FIPS test failed (Figure 2). When you click on OK, the client exits.

Figure 2 Self test failure



FIPS 140-2 startup self test failed.
See the log for further details.

Self integrity check

Loaded application modules (such as Extranet.exe) can only run from the installation directory. This is to validate that the module on disk is the same as the one that is currently running.

For driver files (ipsecw2k.sys and eacfilt.sys), the on disk file in the window's system32/drivers directory is verified. Windows loads these files from this location so that the load path check is not required.

Known answer tests

The following KATs are be performed by the client application during startup:

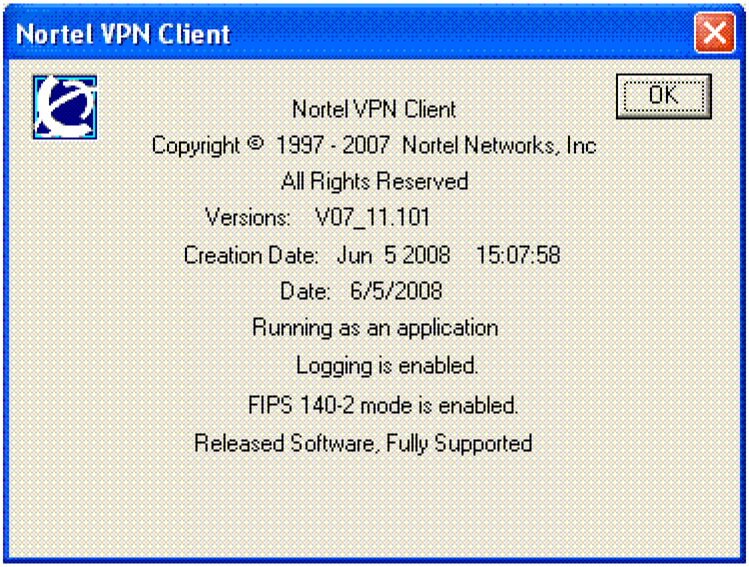
- 3DES
- AES(128 Bit)
- AES(256 Bit)
- SHA1
- HMAC-SHA1
- DH group 2 and 5
- PRNG

The driver runs its own KAT to verify the integrity of its encryption algorithms. If the test fails, no tunnels will be started.

FIPS mode status

The status of FIPS mode (enabled or disabled) is displayed in two places. In the main dialog, it is displayed in Help About (Figure 3).

Figure 3 Status in Help About



Nortel VPN Client

Copyright © 1997 - 2007 Nortel Networks, Inc

All Rights Reserved

Versions: V07_11.101

Creation Date: Jun 5 2008 15:07:58

Date: 6/5/2008

Running as an application

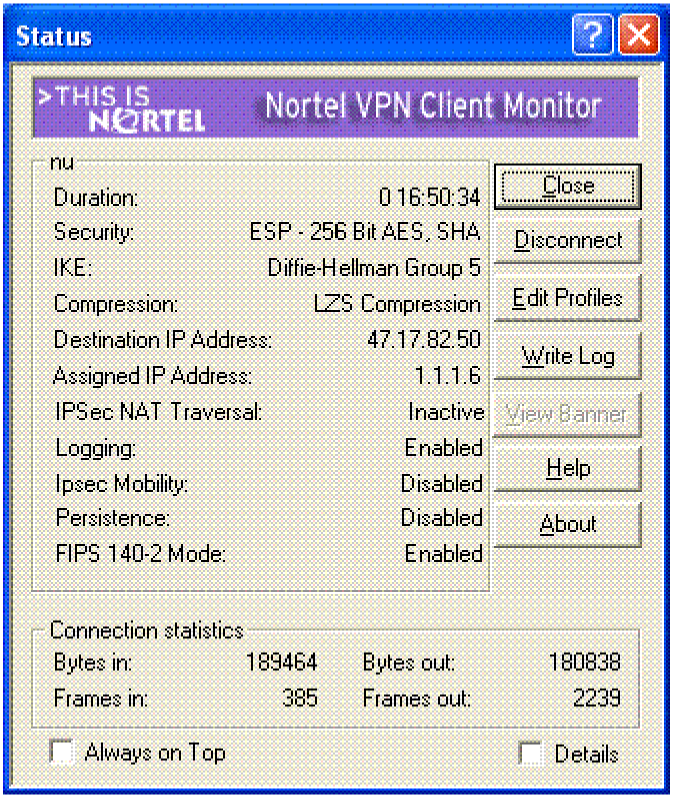
Logging is enabled.

FIPS 140-2 mode is enabled.

Released Software, Fully Supported

Once a tunnel has been established, it also displays in the status box (Figure 4).

Figure 4 Status box



nu

Duration: 0 16:50:34
Security: ESP - 256 Bit AES, SHA
IKE: Diffie-Hellman Group 5
Compression: LZS Compression
Destination IP Address: 47.17.82.50
Assigned IP Address: 1.1.1.6
IPSec NAT Traversal: Inactive
Logging: Enabled
Ipsec Mobility: Disabled
Persistence: Disabled
FIPS 140-2 Mode: Enabled

Connection statistics

Bytes in:	189464	Bytes out:	180838
Frames in:	385	Frames out:	2239

☐ Always on Top ☐ Details

Continuous random number generator (RNG) test

FIPS requires that the RNG be continuously monitored to ensure it returns changing values. If RNG fails, the tunnel will be torn down.

Split tunneling mode

When FIPS mode is enabled, split-tunneling (both normal and inverse) is not allowed. If the server does send split tunneling routes during config mode, that information is ignored. The tunnel comes up but runs in mandatory tunneling mode. If this occurs, the following log entries are made:

```
Wed Dec 10 05:50:29 2008 | FIPS | W | Server is configured
for split tunneling but that is not allowed in FIPS mode.
Wed Dec 10 05:50:29 2008 | ConfMode | I | Mandatory
tunneling enforced.
```

The Nortel gateway continues as though the client is performing split-tunneling. It drops any packets that it determines should not have been sent through the tunnel. Even though the tunnel is established, the expected connectivity may not be there.

It is recommended that you configure groups for FIPS users or the server for mandatory tunneling.

Logging

Logging is mandatory in FIPS mode. The logging option under the Options, Log Sessions to File is checked to indicate that it is active and grayed out to prevent you from changing it.

The log contains the status of the FIPS mode and the results of the KAT and integrity checks.

```
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2 mode is
enabled.
Wed Dec 10 05:45:52 2008 | Isakmp | I | NVC Product Version
- V07_11.101
Wed Dec 10 05:45:52 2008 | Isakmp | I | Drivers' versions -
ipsecw2k.sys:7.11.0.101
; eacfilt.sys:7.11.0.101
Wed Dec 10 05:45:52 2008 | Isakmp | I | NVC executable
Version - 7.11.0.101
Wed Dec 10 05:45:52 2008 | Isakmp | I | Logging subsystem
initialized.
Wed Dec 10 05:45:52 2008 | Isakmp | I | Nortel VPN Client
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file: C:\Program Files\Nortel\Nortel VPN
Client\extranet.exe
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file: C:\Program Files\Nortel\Nortel VPN
Client\certal.dll
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file:
C:\WINDOWS\system32\drivers\ipsecw2k.sys
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Hash
verification OK for file:
C:\WINDOWS\system32\drivers\eacfilt.sys
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: Triple DES
KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: AES (128
Bits) KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: AES (256
Bits) KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: SHA1 KAT
passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2: HMAC-SHA1
KAT passed.
Wed Dec 10 05:45:52 2008 | FIPS | I | FIPS 140-2:
Diffie-Hellman Group 2 KAT passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2:
Diffie-Hellman Group 5 KAT passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2: PRNG KAT
passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2: Eacfilt
```

```
driver HMAC-SHA1 KAT and Integrity test passed.
Wed Dec 10 05:45:53 2008 | FIPS | I | FIPS 140-2: Ipsec
driver Triple DES, AES(128 Bits and 256 Bits), SHA1,
HMAC-SHA1 KAT passed.
Wed Dec 10 05:45:53 2008 | Isakmpd | I | Session End
Notification setup for XP :.
```

Supported DH groups and ciphers

The proposals made by the client in FIPS mode are, in order:

1. DH group 5: AES256-SHA1, AES128-SHA1.
2. DH group 2: 3DES-SHA1, AES128-SHA1.

The AesDisabled setup.ini is supported. If you set it along with FIPS mode, the client only proposes the group 2-3DES transform.

The following are not supported when running in FIPS mode:

- Diffie-Hellman group 8
- DES and DH group 1
- 40-bit DES
- MD5
- IPSEC AH

When you are running in FIPS mode, these will not be proposed by the client. The client rejects any proposal from the server that includes one of the unsupported groups or algorithms.

RSA and MSCAPI

The MSCAPI validates signatures when RSA certificates are used for authentication. To conform to FIPS, the client security policy states which versions of the Microsoft library have been FIPS-approved. The MSCAPI functions are provided by the rsaenh.dll library.

Disabling FIPS mode

Nortel VPN client version 7.11 operates in FIPS mode by default. To disable this mode, you have to run the custom install with the option NN_FIPSMODE=0.

For information on how to customize this installation, refer to *Nortel VPN Router Configuration — Client Version* 7.01 (NN46110-306) 311644-K Rev 02.

Index

A

acronyms 10

C

ciphers 23

conventions, text 9

cryptographic components 17

D

DH groups 23

disabling FIPS 24

F

FIPS mode
  defined 17

FIPS operating mode. *See* FIPS mode

L

logging 21

M

MSCAPI 23

N

normal operating mode 17

Nortel VPN clients
  operating modes 17

O

operating modes, Nortel VPN client 17

P

publications
  hard copy 11
  related 11

S

self tests
  initialization 18
  integrity check 18
  known answer 19
  RNG 20

self-tests 17

split tunneling 21

status 19

T

technical publications 11

text conventions 9